



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/787,784	07/30/2001	Rodney Perkins	RJENK22.001APC	7506
20995 7590 04/24/2009 KNOBBE MARTENS OLSON & BEAR LLP 2040 MAIN STREET FOURTEENTH FLOOR IRVINE, CA 92614				
EXAMINER				
SHERR, CRISTINA O				
ART UNIT		PAPER NUMBER		
3685				
NOTIFICATION DATE		DELIVERY MODE		
04/24/2009		ELECTRONIC		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

jcartee@kmob.com
eOAPilot@kmob.com

Notice of Allowability**Application No.**

09/787,784

Examiner

CRISTINA OWEN SHERR

Applicant(s)

PERKINS, RODNEY

Art Unit

3685

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERIT IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to amendment, filed 06/30/08.
2. ☒ The allowed claim(s) is/are 31-50.
3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some* c) ☐ None of the:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. ____.
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: ____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
- (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
- 1) ☐ hereto or 2) ☐ to Paper No./Mail Date ____.
- (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date ____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date ____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413),
Paper No./Mail Date ____
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other ____.

CRISTINA OWEN SHERR

Examiner

Art Unit: 3685

1. This Office Action is in response to Applicant's amendment, filed January 9, 2009.

EXAMINER'S AMENDMENT

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the issue fee.
3. Authorization for this examiner's amendment was given in a telephone interview with John M. Carson, reg. no. 34,303 on March 5, 2009.
4. Claims 9-30 are hereby canceled. Claims 31-50 are newly added as follows:

31. A data transfer system, comprising:

a sender facility, comprising a sender computer system;

a key facility, comprising a key computer system;

a receiver facility, comprising a receiver computer system,

wherein the sender facility further comprises:

a sender computer readable medium in the sender computer system, the sender computer readable medium comprising instructions which, when executed, cause the sender computer system to:

encrypt data, wherein the encrypted data comprises a first encrypted part and a second encrypted part;

generate a third encrypted part by encrypting the first encrypted part;

generate a data block by combining the third encrypted part with the second encrypted part; and

transmit the data block to the receiver facility,

wherein the receiver facility further comprises:

a receiver computer readable medium in the receiver computer system, the receiver computer readable medium comprising instructions which, when executed, cause the receiver computer system to:

receive the data block;

split the data block into the third encrypted part and the second encrypted part;

generate a request for the key facility to recover the first encrypted part by decrypting the third encrypted part, wherein the request comprises the third encrypted part;

transmit the request to the key facility;

receive the first encrypted part from the key facility; and

decrypt the second encrypted part with the first encrypted part,

wherein the key facility further comprises:

a key computer readable medium in the key computer system, the key computer readable medium comprising instructions which, when executed, cause the key computer system to:

receive the request from the receiver facility;

recover the first encrypted part by decrypting the third encrypted part; and

transmit the first encrypted part to the receiver facility.

32.(New) The system of Claim 31, wherein the instructions of the sender facility, when executed further cause the sender computer system to sign the data block.

33.(New) The system of Claim 31, wherein the instructions of the sender facility, when executed further cause the sender computer system to transmit the data block to the key facility, and wherein the instructions of the key facility, when executed further cause the key computer system to receive the data block and to forward the data block to the receiver facility.

34. (Currently Amended) The system of Claim 33, wherein the instructions of the key facility, when executed further cause the key computer system to log receipt of the data block.

35. (New) The system of Claim 31, wherein the instructions of the key facility, when executed further cause the key computer system to log receipt of the third encrypted part.

36. (New) The system of Claim 31, wherein the instructions of the key facility, when executed further cause the key computer system to log receipt of the request for recovery of the first encrypted part as proof of delivery of the data block to the receiver facility.

37. (New) The system of Claim 36, wherein the instructions of the sender facility, when executed further cause the sender computer system to request proof of delivery information from the key facility.

38. (New) The system of Claim 31, wherein the key facility is a trusted third party.

39. (New) A method of data transfer, the method comprising:

- by a sender facility computer system, encrypting data, wherein the encrypted data comprises a first encrypted part and a second encrypted part;

- by the sender facility computer system, generating a third encrypted part by encrypting the first encrypted part;

- by the sender facility computer system, generating a data block by combining the third encrypted part with the second encrypted part;

- by the sender facility computer system, transmitting the data block to a receiver facility computer system;

- by the receiver facility computer system, receiving the data block;

- by the receiver facility computer system, splitting the data block into the third encrypted part and the second encrypted part;

- by the receiver facility computer system, transmitting a request for the key facility computer system to recover the first encrypted part by decrypting the third encrypted part, the request comprising the third encrypted part;

by the key facility computer system, recovering the first encrypted part by decrypting the third encrypted part;

by the key facility computer system, transmitting the first encrypted part to the receiver facility computer system; and

by the receiver facility computer system, decrypting the second encrypted part with the first encrypted part.

40. (New) The method of Claim 39, further comprising at the sender facility computer system, signing the data block.

41. (New) The method of Claim 39, further comprising at the sender facility computer system, transmitting the data block to the key facility computer system, and at the key facility computer system, receiving the data block and forwarding the data block to the receiver facility computer system.

42. (New) The method of Claim 41, further comprising, at the key facility computer system, logging receipt of the data block.

43. (New) The method of Claim 39, further comprising at the sender facility computer system, transmitting the data block to the receiver facility computer system, and at the receiver facility computer system, receiving the data block.

44. (New) The method of Claim 43, further comprising, at the key facility computer system, logging receipt of the third encrypted part.

45. (New) The method of Claim 39, further comprising, at the key facility computer system, logging receipt of the request for decryption of the third encrypted part as proof of delivery of the data block to the receiver facility computer system.

46. (New) The method of Claim 45, further comprising, at the sender facility computer system, requesting proof of delivery information from the key facility computer system.

47. (New) The method of Claim 39, wherein the key facility computer system is a trusted third party.

48. (New) A data transfer system comprising:

a sender facility, comprising a sender computer system;

a key facility, comprising a key computer system;

a receiver facility, comprising a receiver computer system,
wherein the sender facility comprises:

a sender computer readable medium in the sender computer system, the sender computer readable medium comprising instructions which, when executed, cause the sender computer system to:

encrypt data, wherein the encrypted data comprises a plurality of encrypted parts, the plurality of encrypted parts comprising at least one first encrypted part and one or more second encrypted parts;

generate a further encrypted part by encrypting the at least one first encrypted part;

generate a data block by combining the further encrypted part and the second encrypted parts;

sign the data block;

transmit the data block to the key facility; and

request proof of delivery information from the key facility,

wherein the receiver facility comprises:

a receiver computer readable medium in the receiver computer system, the receiver computer readable medium comprising instructions which, when executed, cause the receiver computer system to:

receive the data block from the key facility;

generate a request for the key facility to recover the at least one first encrypted part by decrypting the further encrypted part;

transmit the request to the key facility;

receive the at least one first encrypted part from the key facility; and

decrypt the one or more second encrypted parts with the at least one first encrypted part,

wherein the key facility further comprises:

a key computer readable medium in the key computer system, the key computer readable medium comprising instructions which, when executed, cause the key computer system to:

- receive the data block from the sender facility;
- forward the data block to the receiver facility;
- log receipt of the data block from the sender facility;
- log receipt of the decryption request from the receiver facility as proof of delivery of the data block to the receiver facility;
- recover the at least one first encrypted part by decrypting the further encrypted part; and
- transmit the recovered at least one first encrypted part to the receiver facility.

49.(New) A data transfer system, comprising:

- a sender facility, comprising a sender computer system;
- a key facility, comprising a key computer system;
- a receiver facility, comprising a receiver computer system,

wherein the sender facility further comprises:

- a sender computer readable medium in the sender computer system, the sender computer readable medium comprising instructions which, when executed, cause the sender computer system to:

- encrypt data, wherein the encrypted data comprises a plurality of encrypted parts, the plurality of encrypted parts comprising at least one first encrypted part and one or more second encrypted parts;

- produce a further encrypted part by encrypting the at least one first encrypted part;

- produce a data block by combining the further encrypted part and the second encrypted parts;

- sign the data block; and

- transmit the data block to the receiver facility,

wherein the receiver facility further comprises:

- a receiver computer readable medium in the receiver computer system, the receiver computer readable medium comprising instructions which, when executed, cause the receiver computer system to:

- receive the data block from the sender facility;
- generate a request for the key facility to recover the at least one first encrypted part by decrypting the further encrypted part, wherein the request comprises the further encrypted part;
- transmit the request to the key facility;
- receive the at least one first encrypted part from the key facility; and
- decrypt one or more second encrypted parts with at the at least one first encrypted part,

wherein the key facility further comprises:

- a key computer readable medium in the key computer system, the key computer readable medium comprising instructions which, when executed, cause the key computer system to:
 - log receipt of the further encrypted part;
 - recover the at least one first encrypted part by decrypting the further encrypted part; and
 - transmit the first encrypted part to the receiver facility.

50.(New) A method of transferring data, comprising:

- by a sender facility computer system, encrypting data, wherein the encrypted data comprises a plurality of encrypted parts, the plurality of encrypted parts comprising at least one first encrypted part and one or more second encrypted parts;
- by the sender facility computer system, generating a further encrypted part by encrypting the at least one first encrypted part;
- by the sender facility computer system, producing a data block by combining the further encrypted part and a second encrypted part;
- by the sender facility computer system, signing the data block;
- by the sender facility computer system, sending the data block to a key facility computer system;
- by the key facility computer system, receiving the data block from the sender facility computer system;

by the key facility computer system, forwarding the data block to a receiver facility computer system;

by the key facility computer system, logging receipt of the data block from the sender facility computer system;

by the receiver facility computer system, receiving the data block from the key facility computer system;

by the receiver facility computer system, generating a request for the key facility computer system to recover the first encrypted part by decrypting the further encrypted part;

by the receiver facility computer system, transmitting the request to the key facility computer system;

by the key facility computer system, logging receipt of the request from the receiver facility computer system as proof of delivery of the data block to the receiver facility computer system;

by the key facility computer system, recovering the first encrypted part by decrypting the further encrypted part;

by the key facility computer system, sending the first encrypted part to the receiver facility computer system;

by the key facility computer system, decrypting the one or more second encrypted parts with the first encrypted part; and

by the sender facility computer system, requesting proof of delivery information from the key facility computer system.

Reasons for Allowance

The following is the Examiner's statement of reasons for allowance:

4. Regarding the claimed terms, the Examiner notes that a "general term must be understood in the context in which the inventor presents it." *In re Glaug* 283 F.3d 1335,

1340, 62 USPQ2d 1151, 1154 (Fed. Cir. 2002). Therefore the Examiner must interpret the claimed terms as found on pages 1-24 of the specification. Clearly almost all the general terms in the claims may have multiple meanings. So where a claim term "is susceptible to various meanings . . . the inventor's lexicography must prevail" *Id.* Using these definitions for the claims, the claimed invention was not reasonably found in the prior art.

5. Regarding the independent claims 31, 39, 48, 49, and 50, the primary reference, Ginter, discloses as previously discussed. Ginter, however, does not disclose that the receiver facility receives the encrypted data from the key facility and then requests that the key facility decrypt the data thus returning the data to the key facility. Moreover, the missing elements of Ginter are not likely found in a reasonable number of reference(s).

6. Yet even if the missing claimed elements were found in a reasonable number of references, a person of ordinary skill in the art at the time the invention was made would not have been motivated to include these missing elements in an embodiment of Ginter, since normally one would not seek to return the data to where it came from.

7. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to CRISTINA OWEN SHERR whose telephone number is

(571)272-6711. The examiner can normally be reached on 8:30-5:00 Monday through Friday.

9. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Calvin L. Hewitt, II can be reached on (571)272-6709. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

10. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Cristina Owen Sherr
Patent Examiner, AU 3685

/Calvin L Hewitt II/

Supervisory Patent Examiner, Art Unit 3685